

REMARKS

STATUS OF CLAIMS

Claims 1, 2 and 5-28 are pending.

Claims 7, 13-16, 18-27, 29-33, 35 and 37-38 are withdrawn.

Claims 1, 2, 5-6, 8-12, 17, 28, 34 and 36 are rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Hashimoto et al., U.S. Patent Publication No. 2001/0018736 (hereinafter "Hashimoto").

In accordance with the foregoing, the claim are amended, and, thus, the pending claims remain for reconsideration, which is respectfully requested.

No new matter has been added.

The Examiner's rejections are respectfully traversed.

CLAIM REJECTIONS:

Independent claims 1, 28, 34 and 36 are allegedly unpatentable over Hashimoto

In accordance with the foregoing, claim 1 is amended to recite, in part: "an encrypting unit obtaining, from a first Generic Tamper resistant module license (GT license) of a first program, an access condition for accessing a memory region during an execution process of the first program and a code decryption key for decrypting an encrypted block configuring the first program, by decrypting with the first private key the first GT license of the first program encrypted with a public key pairing with the first private key." Support for the claim amendment can be found, for example, at page 42, lines 10-17 of the Application specification.

The Office Action, at page 3, relies upon Hashimoto, at paragraphs 74 and 75 to disclose the same.

Paragraphs 74 and 75 of Hashimoto recite:

[0074] (1) A common key K_x selected by a program creator. The application program will be encrypted by the secret key cryptosystem using this key.

[0075] (2) A pair of a unique public key K_p and a unique secret key K_s provided inside the processor. The public key can be read out by the program by using instructions.

[0076] (3) An encryption key information in which the common key K_x of the program is encrypted by using the public key K_p of the processor.

In other words, Hashimoto discusses a public key K_p is paired with a secret key K_S

provided in a processor, and that a common key Kx is encrypted by using the public key Kp. The Office Action at page 3, asserts Hashimoto's common key Kx in paragraph 74 is similar to the claimed "license."

However, Applicants respectfully submit that Hashimoto fails to disclose, either expressly or implicitly, the claimed "an encrypting unit **obtaining, from a first Generic Tamper resistant module license (GT license)** of a first program, **an access condition** for accessing a memory region during an execution process of the first program and **a code decryption key** for decrypting an encrypted block configuring the first program, by decrypting with the first private key the first GT license of the first program encrypted with a public key pairing with the first private key," because Hashimoto fails to disclose, either expressly or implicitly, the claimed GT license, and, furthermore, Hashimoto merely discusses that a common key Kx is encrypted by using a public key Kp. In other words, the claimed "GT license" differs from Hashimoto's common key Kx. In particular, the claimed "GT license" has, for example, "an access condition" and a "decryption key." One description of the GT license can be found, for example, at page 42, lines 10-17 of the Application Specification.

Accordingly, Applicant's respectfully submit that a *prima facie* case of obviousness cannot be based upon Hashimoto, because there is no evidence that one skilled in the art would modify Hashimoto's common key Kx to provide the claimed "**first Generic Tamper resistant module license (GT license)** of a first program, [having] **an access condition** for accessing a memory region during an execution process of the first program and **a code decryption key** for decrypting an encrypted block configuring the first program," and seen a benefit of, for example, having "not only general versatility equivalent to a software TRM, but also safety equivalent to a hardware TRM" (see the Application specification, at page 4, lines 20-22).

Furthermore, Applicants respectfully request that in any response to this amendment, which does not allow the claims, the Examiner specifically provide a citation in the reference which discloses the claimed "encrypting unit **obtaining, from a first Generic Tamper resistant module license (GT license)** of a first program, **an access condition** for accessing a memory region during an execution process of the first program and **a code decryption key** for decrypting an encrypted block configuring the first program, by decrypting with the first private key the first GT license of the first program encrypted with a public key pairing with the first private key" and provide a rational basis for supporting the rejection.

Applicants respectfully submit that independent claims 28, 34 and 36 patentably distinguish over the art of record for similar reasons as independent claim 1.

Dependent claims recite patentably distinguishing features of their own or are at least patentably distinguishing due to their dependence from the independent claims. Withdrawal of the rejection of pending claims, and allowance of pending claims is respectfully requested.

CONCLUSION

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.


Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: December 21, 2007

By: 
Matthew H. Polson
Registration No. 58,841

1201 New York Avenue, N.W., 7th Floor
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501